

## How to Deploy an F-Series Firewall in Microsoft Azure using Azure Portal and ARM

<https://campus.barracuda.com/doc/48202653/>

If you are in a region, where the Azure Marketplace is not available, download VHD disk images from the [Barracuda Download portal](#) and deploy the firewall via user defined images.

For more information, see [How to Upload Azure VHD Images for User Defined Images using ARM](#) and [How to Deploy an F-Series Firewall in Microsoft Azure using PowerShell and ARM](#).

The Barracuda NextGen Firewall F-Series for Microsoft Azure can be deployed as a virtual machine in the Microsoft Azure cloud. You can choose between the following images in the Azure Marketplace:

- **Barracuda NextGen Firewall F-Series (BYOL)** - These images use licenses purchased directly from Barracuda Networks. Barracuda Networks offers a 30-day evaluation license.
- **Barracuda NextGen Firewall F-Series (PAYG)** - These images do not need to be licensed separately. Licensing fees are included in the hourly price of the Instance. All charges are billed directly through your Microsoft Azure account.
- **Barracuda NextGen Control Center for Microsoft Azure (BYOL)** - These images use licenses purchased directly from Barracuda Networks. Barracuda Networks offers a 30-day evaluation license.

Depending on your deployment, you may want to use more than one resource group to be able to maintain the deployed VMs more easily.

### Video

Watch the following video of a NextGen Firewall PAYG deployment via the Azure portal. After the firewall is up and running the firewall is configured to act as the default gateway for the backend resources.

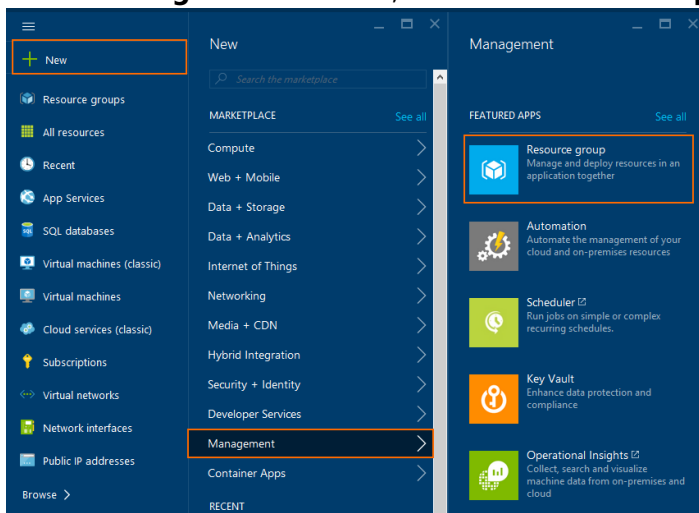


## Before you begin

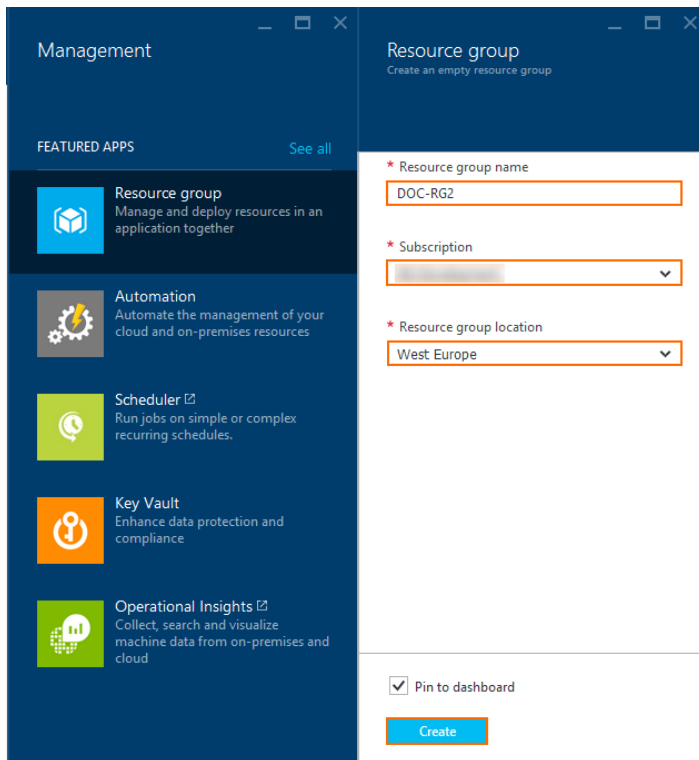
- Create a [Microsoft Azure account](#).
- (BYOL images only) Purchase a Barracuda NextGen Firewall F-Series or Control Center for Microsoft Azure license, or register to receive an evaluation license from the [Barracuda Networks Evaluation page](#).

## Step 1. Create a resource group

1. Go to the Azure Portal: <https://portal.azure.com>
2. In the upper left-hand corner, click **NEW**.
3. In the **NEW** column, click **Management**.
4. In the **Management** column, click **Resource Group**.



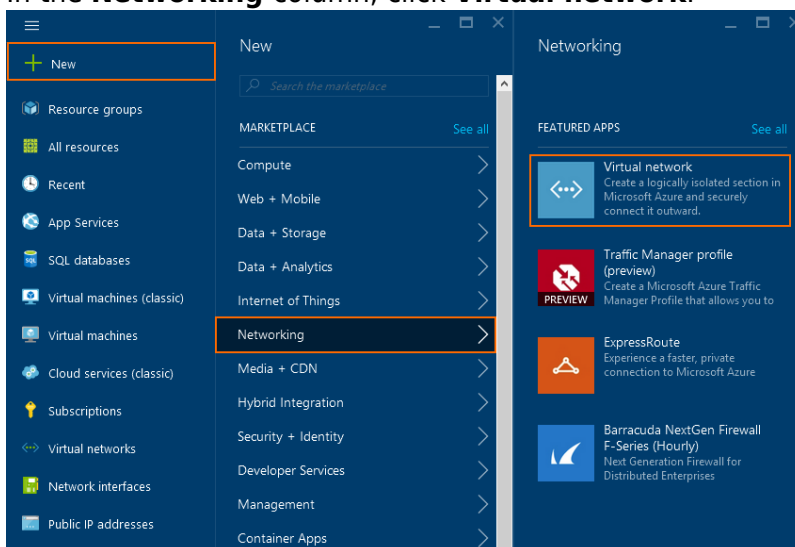
5. In the **Resource Group** column, enter:
  - **Resource group name** – Enter a unique name for your resource group.
  - **Subscription** – Select the Azure Subscription.
  - **Resource group location** – Select the Azure datacenter where you want to deploy your VM. All resources in the resource group must be in the same location.



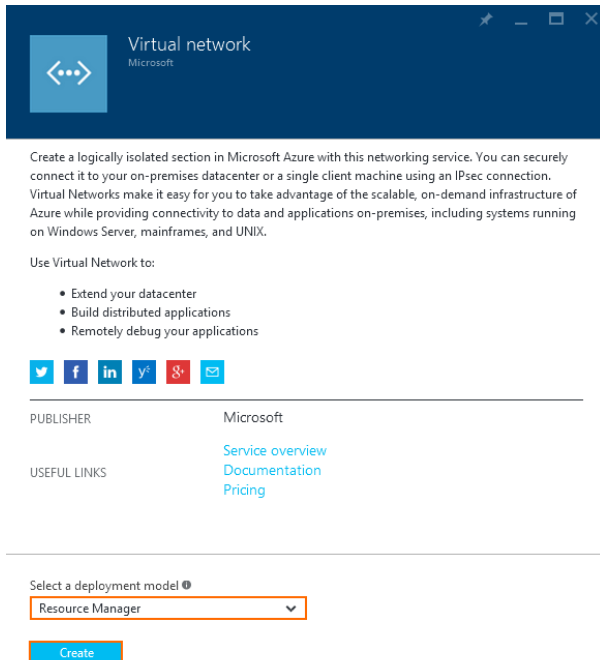
6. Click **Create**.

## Step 2. Create a virtual network

1. Go to the Azure Portal: <https://portal.azure.com>
2. In the upper left-hand corner, click **NEW**.
3. In the **NEW** column, click **Networking**.
4. In the **Networking** column, click **Virtual network**.



5. In the **Virtual network** column, select **Resource Manager** from the **deployment model** drop-down list.



Virtual network  
Microsoft

Create a logically isolated section in Microsoft Azure with this networking service. You can securely connect it to your on-premises datacenter or a single client machine using an IPsec connection. Virtual Networks make it easy for you to take advantage of the scalable, on-demand infrastructure of Azure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes, and UNIX.

Use Virtual Network to:

- Extend your datacenter
- Build distributed applications
- Remotely debug your applications

PUBLISHER: Microsoft

USEFUL LINKS: [Service overview](#), [Documentation](#), [Pricing](#)

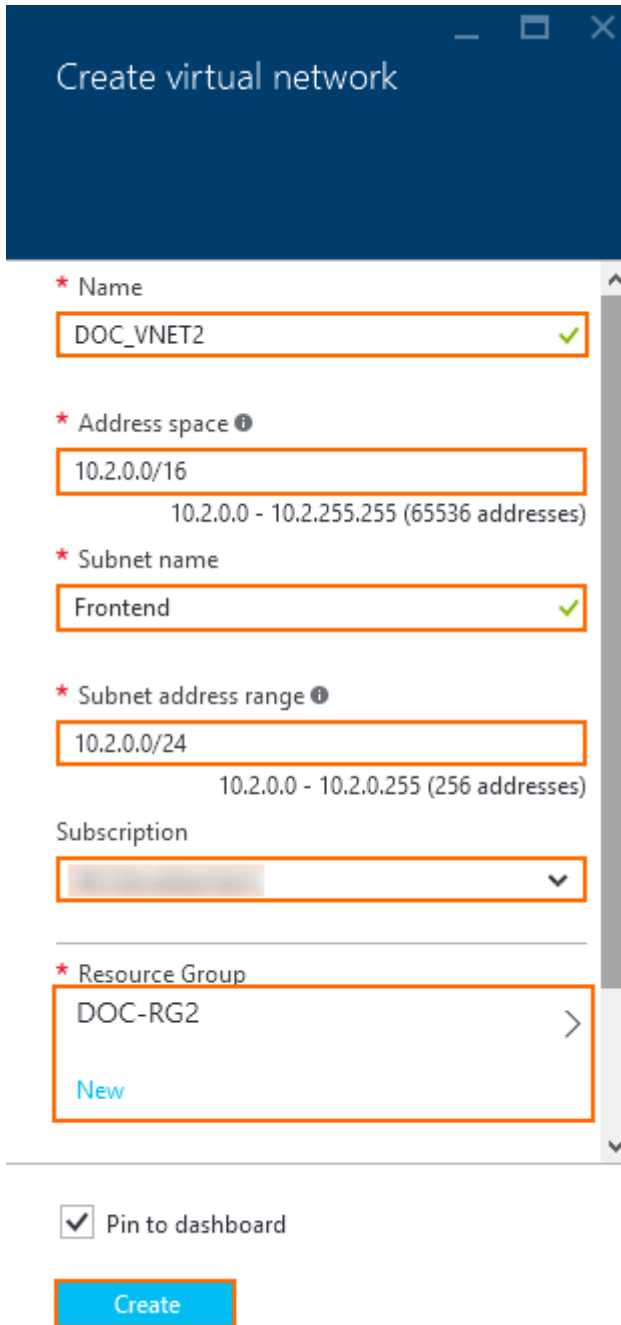
Select a deployment model: Resource Manager

Create

6. Click **Create**.

7. In the **Create virtual network** column, enter:

- **Name** – Enter a unique name for the virtual network.
- **Address space** – Use a large network not overlapping with your on-premise networks.
- **Subnet name** – Enter a name for the first subnet in the virtual network. E.g., Frontend
- **Subnet address range** – Enter the network for the subnet. It must be a subnet of the network entered as the address space.
- **Subscription** – Select the Azure subscription.
- **Resource Group** – Click **Select Existing** and select the resource group created in step 1.
- **Location** – Select the location the resource group is in.



Create virtual network

\* Name  
DOC\_VNET2 ✓

\* Address space ⓘ  
10.2.0.0/16  
10.2.0.0 - 10.2.255.255 (65536 addresses)

\* Subnet name  
Frontend ✓

\* Subnet address range ⓘ  
10.2.0.0/24  
10.2.0.0 - 10.2.0.255 (256 addresses)

Subscription  
▼

\* Resource Group  
DOC-RG2 >  
New

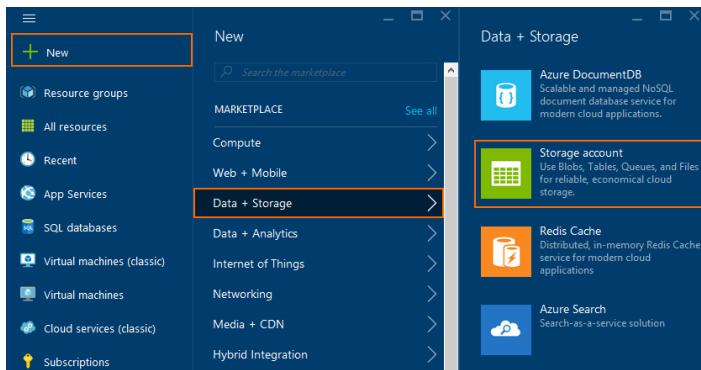
Pin to dashboard

Create

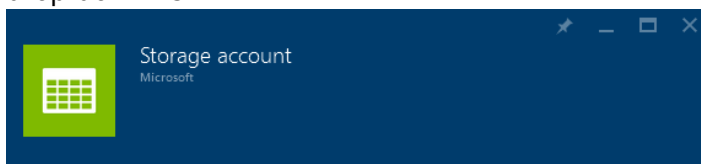
8. Click **Create**.

### Step 3. Create a storage account

1. Go to the Azure Portal: <https://portal.azure.com>
2. In the upper left-hand corner, click **NEW**.
3. In the **NEW** column, click **Data + Storage**.
4. In the **Data + Storage** column, click **Storage account**.



5. In the **Storage account** column, select **Resource Manager** from the **deployment model** drop-down list.



Microsoft Azure provides scalable, durable cloud storage, backup, and recovery solutions for any data, big or small. It works with the infrastructure you already have to cost-effectively enhance your existing applications and business continuity strategy, and provide the storage required by your cloud applications, including unstructured text or binary data such as video, audio, and images.



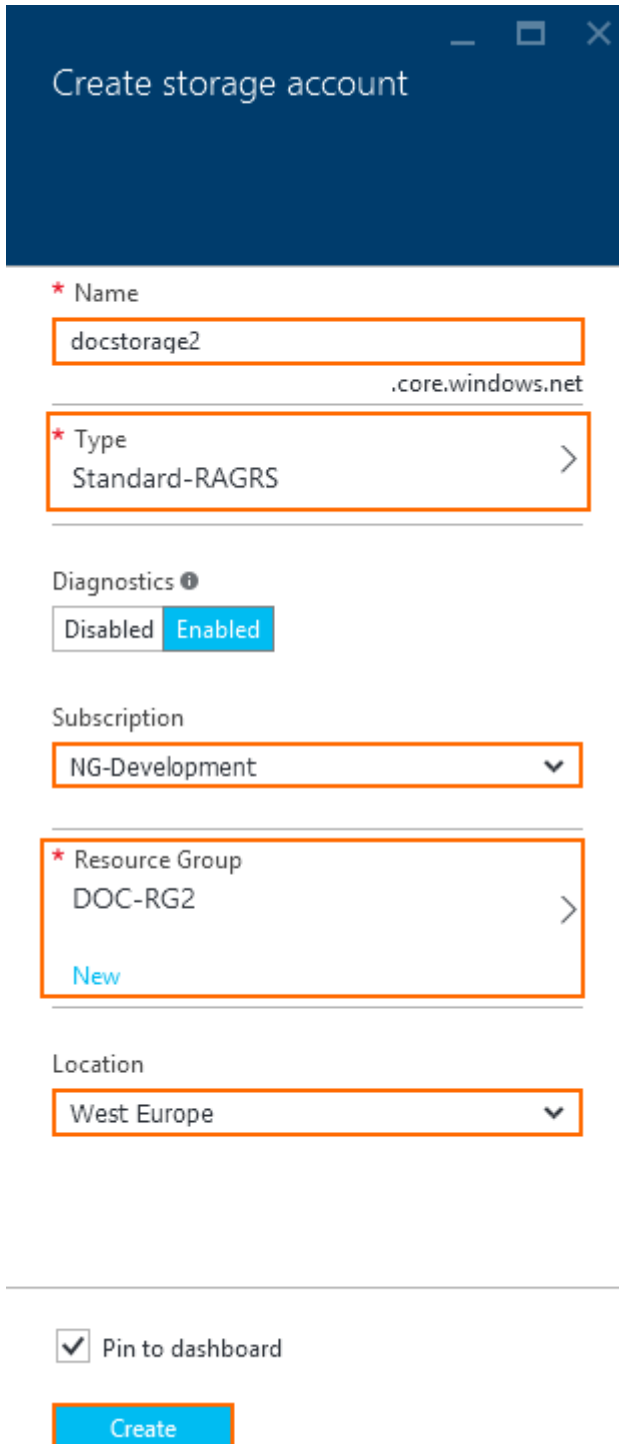
PUBLISHER	Microsoft
USEFUL LINKS	<a href="#">Service overview</a> <a href="#">Documentation</a> <a href="#">Pricing</a>

Select a deployment model 

Resource Manager 

[Create](#)

6. Click **Create**.
7. In the **Create storage account** column, enter:
- **Name** – Enter a unique storage account name.
  - **Type** – Select the storage account type and how it is replicated.
  - **Subscription** – Select the Azure subscription.
  - **Resource Group** – Click **Select Existing** and select the resource group created in step 1.
  - **Location** – Select the location the resource group is in.



Create storage account

\* Name  
docstorage2  
.core.windows.net

\* Type  
Standard-RAGRS

Diagnostics ⓘ  
Disabled Enabled

Subscription  
NG-Development

\* Resource Group  
DOC-RG2  
New

Location  
West Europe

Pin to dashboard

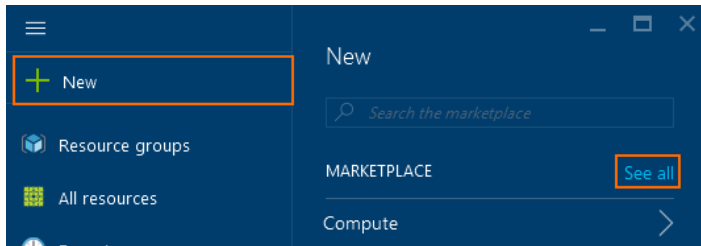
Create

8. Click **Create**.

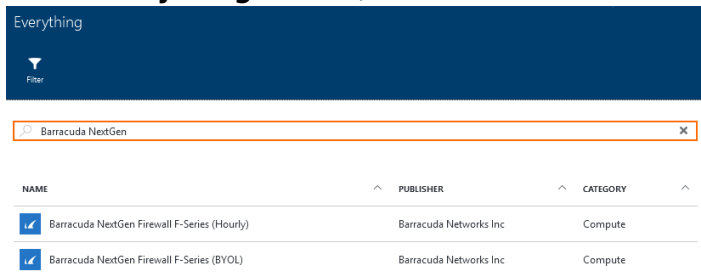
#### Step 4. Deploy the Barracuda NextGen Firewall F-Series VM

1. Go to the Azure Portal: <https://portal.azure.com>
2. In the upper left-hand corner, click **NEW**.

3. In the **NEW** column, next to **MARKETPLACE** click **See all** link.



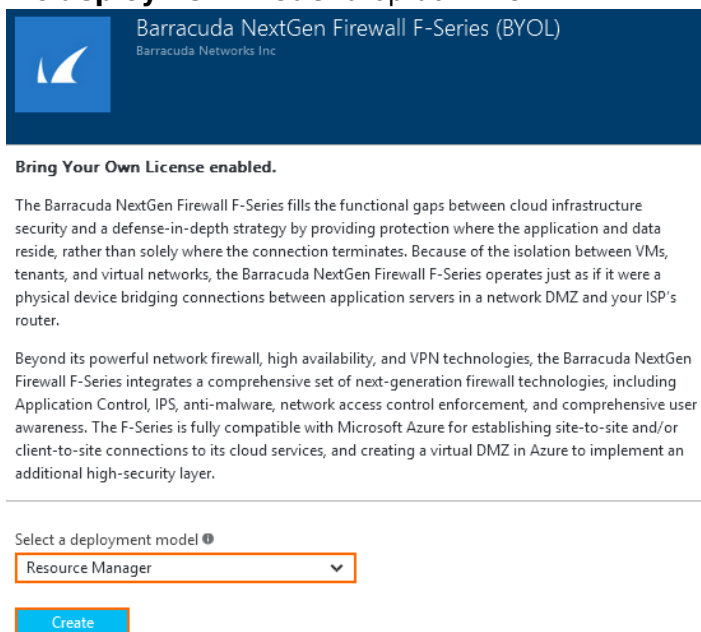
4. In the **Everything** column, search for Barracuda NextGen.



5. Select the image from the list:

- **Barracuda NextGen Firewall F-Series (BYOL)**
- **Barracuda NextGen Firewall F-Series (Hourly)**
- **Barracuda NextGen Control Center for Microsoft Azure (BYOL)**

6. In the **Barracuda NextGen** column for the selected image, select **Resource Manager** from the **deployment model** drop-down list.



7. Click **Create**.

8. In the **Basics** column, configure:

- **Name** – Enter the name of the Barracuda NextGen VM.
- **User name** – Enter a placeholder username to satisfy the Azure input validation. This username is not used.
- **Authentication Type** – Select **Password**.
- **Password** – Enter the root password.



- **Subscription** – Select the Azure subscription.
- **Resource Group** – Click **Select Existing** and select the resource group created in step 1.
- **Location** – Select the location the resource group is in.

The screenshot shows the 'Basics' configuration step of the 'Create virtual machine' wizard. The left sidebar lists five steps: 1. Basics (selected), 2. Size, 3. Settings, 4. Summary, and 5. Buy. The main area contains the following fields:

- Name:** DOC-NG1
- User name:** doesnotmatterisnotused
- Authentication type:** Password (selected), SSH public key
- Password:** [Redacted]
- Subscription:** NG-Development
- Resource group:** DOC-RG2 (with a 'Create new' link below)
- Location:** West Europe

An 'OK' button is located at the bottom of the form.

9. Click **OK**.
10. In the **Choose a size** column, select the instance size. Click **View all** to select from the full Instance list.

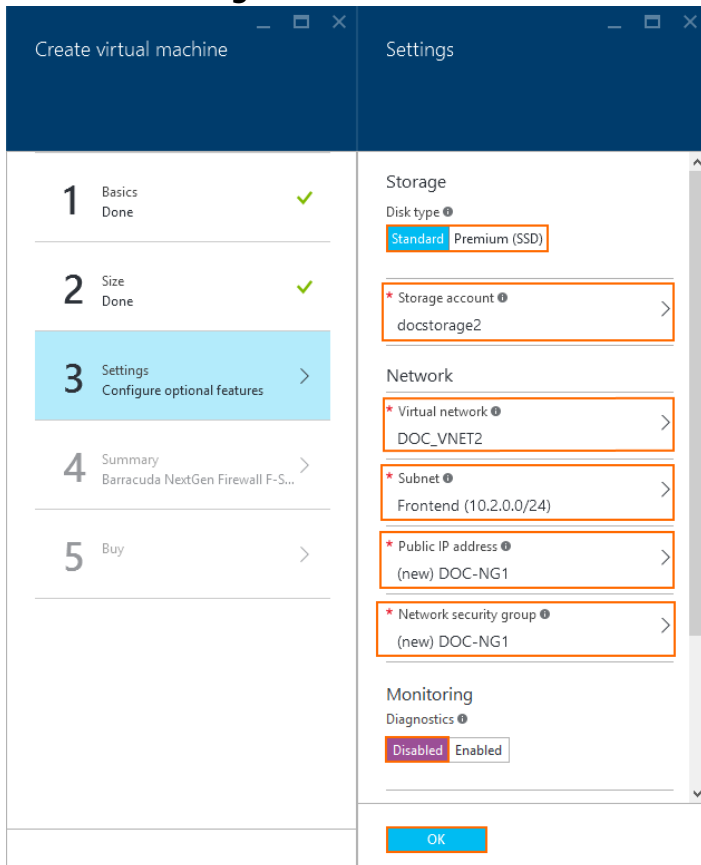
The screenshot shows the 'Choose a size' step of the 'Create virtual machine' wizard. The left sidebar shows step 2 'Size' selected. The main area displays two virtual machine sizes:

A1 Standard	A2 Standard
1 Core	2 Cores
1.75 GB	3.5 GB
2 Data disks	4 Data disks
2x500 Max IOPS	4x500 Max IOPS
Load balancing	Load balancing
Auto scale	Auto scale
44.64 USD/MONTH (ESTIMATED)	89.28 USD/MONTH (ESTIMATED)

A 'Select' button is at the bottom. A 'View all' link is also present.

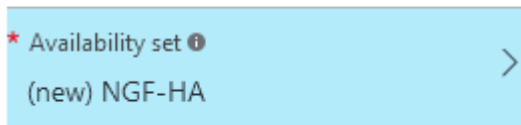
11. Click **Select**.
12. In the **Settings** column, enter the storage, network, and monitoring settings:
  - **Disk type** – Select **standard** for magnetic disks or **Premium (SSD)** for faster SSD-based storage.

- **Storage account** – Select the storage account created in step 3.
- **Virtual network** – Select the virtual network created in step 2.
- **Subnet** – Select the Subnet created in step 2. To use Azure user defined routing, verify that the firewall is not in the same subnet as the backend VMs.
- **Public IP address** – Select a public IP address the VM is reachable through.
- (optional) **Network security group** – Using a network security group is optional. Click and select **none**, or use the default included with the VM.
- **Monitoring** – Click **Disabled**.

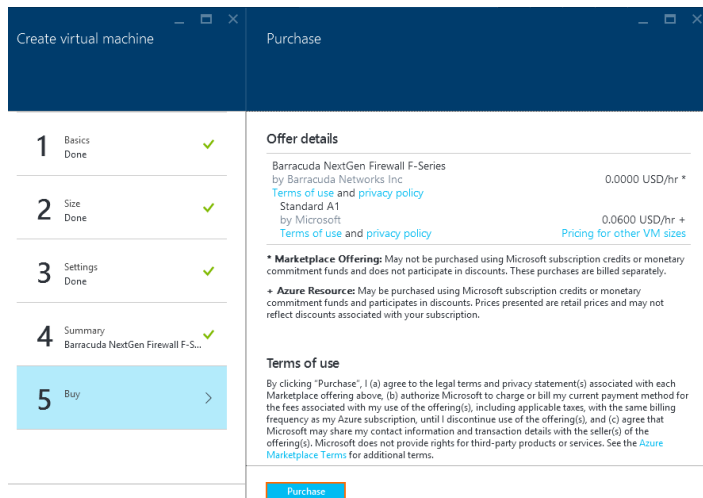


13. (HA Cluster only) In the **Create virtual network** column, add the VM to an **Availability set**:
- **Availability set** – Create a new availability set, or add to an existing availability set.

#### Availability

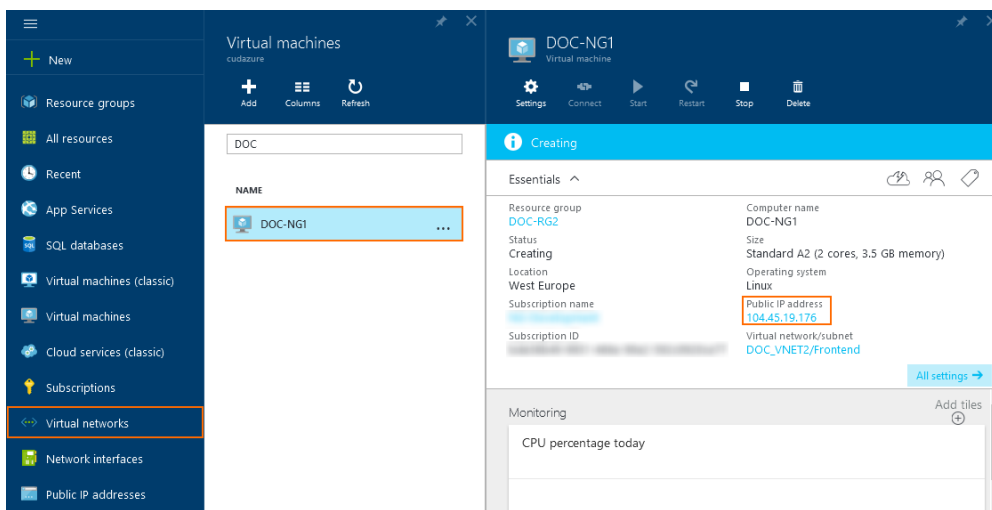


14. Click **OK**.



15. In the **Purchase** column, click **Purchase**.

Wait for Microsoft Azure to finish the deployment of your Barracuda NextGen Firewall F-Series or Barracuda NextGen Control Center. Go to **Virtual machines**, click on the NextGen Firewall VM, and locate the **Public IP address** used to connect to your firewall.



Open the public IP address with your browser for further links on how to download NextGen Admin and how to receive an evaluation license.



The screenshot shows a 'Welcome' page for the Barracuda NextGen Firewall F-series. The page is set against a dark blue background with the Barracuda logo and 'NextGen Firewall F' in white. The main content is in a light grey box with a white background. It includes a 'Welcome' heading, a paragraph of introductory text, a link to an 'Evaluation Request Form', instructions for online activation, a link to the 'NGAdmin.exe' management application, and a note that it requires Windows 7 or later. It also provides links to 'Getting Started' guides for virtual and public cloud editions, and a list of resources including the Barracuda Tech Library, Community Forum, Post-Sales Tech Support, and University website.

**Welcome**

Thank you for deploying Barracuda NextGen Firewall F-series. Unless running in hourly (Pay-As-You-Go) mode, this product requires activation. To test-drive the product with full access to all functions please fill in the evaluation request form, or contact your local Barracuda Networks sales team to obtain an activation token if you have not yet done so. Remember to choose the proper virtual or public cloud edition matching your deployment.

- [Evaluation Request Form](#)

Online activation: Please use the main dashboard in NG Admin application to access activation form once you got the Activation Token.

---

To monitor or manage the configuration for this NextGen Firewall F-series, use the following link to download the management application. For new installations log in as **root** with the password you defined during deployment (or default password **ngf1r3wall** if you have not defined your own).

- [NGAdmin.exe](#)  
(Note: NG Admin requires Windows 7 or later)

---

For additional steps please refer to our Getting Started guides.

- [Getting Started with NextGen Firewall virtual edition](#)
- [Getting Started with NextGen Firewall in public cloud](#)

More documentation, best practice recommendations and implementation guides can be found on Barracuda Tech Library, also feel free to share your experience with other users in Community section of Barracuda Customer Portal. If you need help - simply contact our presales or postsales support teams.

For in depth technical education please visit the Barracuda University website and check out the variety of free online webinars, as well as hands-on seminars to become a certified NextGen Firewall expert.

- [Barracuda Tech Library](#)
- [Barracuda Community Forum](#)
- [Barracuda Post-Sales Tech Support Contacts Worldwide](#)
- [Barracuda University](#)

## Next steps

Configure a user defined routing table for the backend VMs to send traffic through the firewall, and enable Azure Cloud Integration to allow the firewall VM to directly connect to the Azure service fabric.

For more information, see [How to Configure Azure Route Tables \(UDR\) using Azure Portal and ARM](#) and [How to Configure Azure Cloud Integration using ARM](#).

## Figures

1. azure\_deploy\_single\_ui\_01.png
2. azure\_deploy\_single\_ui\_02.png
3. azure\_deploy\_single\_ui\_03.png
4. azure\_deploy\_single\_ui\_04.png
5. azure\_deploy\_single\_ui\_05.png
6. azure\_deploy\_single\_ui\_06.png
7. azure\_deploy\_single\_ui\_07.png
8. azure\_deploy\_single\_ui\_08.png
9. azure\_deploy\_single\_ui\_10.png
10. azure\_deploy\_single\_ui\_11.png
11. azure\_deploy\_single\_ui\_12.png
12. azure\_deploy\_single\_ui\_13.png
13. azure\_deploy\_single\_ui\_14.png
14. azure\_deploy\_single\_ui\_15.png
15. azure\_deploy\_single\_ui\_05a.png
16. azure\_deploy\_single\_ui\_16.png
17. azure\_deploy\_single\_ui\_17.png
18. cloud\_landing\_page.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.